UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

-against-

MICHAEL METTER, STEVEN MOSKOWITZ, ANDREW TEPFER, also known as "Avi," SEYMOUR EISENBERG, also known as "Jimmy, " GEORGE SPERANZA, THOMAS CAVANAGH, and FRANK NICOLOIS,

Defendants.

**Index No.: 1:10-cr-0600-DLI**

**MEMORANDUM OF LAW IN SUPPORT OF MOTION TO SUPPRESS SEIZED PROPERTY**

Hinshaw & Culbertson LLP
780 Third Avenue, 4th Floor
New York, New York 10017
*Attorneys for Defendant Michael Metter*

**TABLE OF CONTENTS**

# TABLE OF AUTHORITIES

**Page(s)**

**CASES**

**OTHER AUTHORITIES**

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>-against-<br><br>MICHAEL METTER, STEVEN MOSKOWITZ, ANDREW TEPFER, also known as "Avi," SEYMOUR EISENBERG, also known as "Jimmy, " GEORGE SPERANZA, THOMAS CAVANAGH, and FRANK NICOLOIS,<br><br>Defendants. | **Index No.: 1:10-cr-0600-DLI** |

**MEMORANDUM OF LAW IN SUPPORT OF MOTION TO SUPPRESS SEIZED PROPERTY**

**Preliminary Statement**

This memorandum is submitted in support of defendant's motion to suppress materials seized from the offices of Spongetech Delivery Systems ("Spongetech"),[1] from the home of Michael Metter, and from an internet services provider ("ISP").[2] In relation to the seizures from Spongetech and from Mr. Metter's home, the warrants authorized the seizure of specified documents, but the government has failed to execute the warrant in a manner that is either

---

1 Defendant Andrew Tepfer joins in this portion of the motion.

2 A corporate officer or employee may assert a reasonable expectation of privacy in the corporate office. United States v. Dupree, 2011 WL 1004824 at *28 (E.D.N.Y. March 18, 2011) (chief operating officer and counsel have standing with respect to searches of corporate premises and records) (citing United States v. Chuang, 897 F.2d 646, 649 (2d Cir. 1990)). *See also* United States v. Burke, 718 F.Supp. 1130, 1135 (S.D.N.Y. 1989) (regarding standing, businessmen have a constitutional right to conduct their business free from unreasonable official entries upon their private property and allegations of indictment regarding operations of business established standing); United States v. Schwimmer, 692 F.Supp. 119, 125 (E.D.N.Y. 1988). Also well established is that an individual has a reasonable expectation of privacy in the contents of his personal email account. *See* United States v. Cioffi, 668 F.Supp.2d 385, 390 n. 7 (E.D.N.Y. 2009).

consistent with its terms or reasonable under the Fourth Amendment. For example, the government imaged and seized not some subset of the electronic records of Spongetech, but instead seized more than 60 hard drives. While the government is permitted to image hard drives as part of its execution of a search warrant, that is permitted *only* as the first step of a two-step process. To comply with the warrant, the government would have then had to conduct an appropriate forensic analysis in order to identify those files that were within the scope of the particular items listed in the warrant. It is perhaps inconvenient to have to actually review the seized materials to identify that which is described in the warrant, but that does not and has never excused adherence to a warrant – whether in large scale seizures of hard copy business records or seizures of electronic files. The government is not permitted to perform only the first half of that process, seizing more than 60 hard drives and then simply keeping them, without regard for their contents.

The government's seizure of all of the contents of more than 60 hard drives from Spongetech was followed by a wholesale seizure of the entire content of Mr. Metter's personal email account. In or about November 2010, the government obtained and executed a search warrant authorizing seizure of the Mr. Metter's personal AOL email account for the period January 2007 through the date of the arrest.[3] Notwithstanding the fact that it was a personal e-mail account, and that the government had ample evidence that Mr. Metter used that address for communications that were confidential, private, privileged and/or entirely unrelated to Spongetech, the government obtained a warrant for seizure of "all" of the contents of the email

---

3 The affidavit of Thomas McGuire in support of the application sought email for the period "until May 4, 2010 to avoid retrieving any potentially privileged emails sent after Metter and Moskowitz obtained counsel." Fritz Aff. at Exhibit 8: McGuire Affidavit at n. 2. Of course, as the government well knew, Mr. Metter had obtained counsel at least 8 months earlier, and had appeared with that counsel to provide testimony to the SEC.

and received and kept all of the contents of that account. Through that seizure, the government in this case appears to have done precisely that which the Fourth Amendment prohibits: taken and kept years worth of Mr. Metter's personal and private communications. From a legal perspective, its seizure is overbroad, its conduct unreasonable, and the materials should be suppressed. From a broader perspective, the government's seizure and retention of Mr. Metter's personal communications and property – particularly its almost nonchalant unlimited seizure of all of his private emails -- is a remarkably invasive and inexcusable repudiation of the Fourth Amendment's protections.

## STATEMENT OF FACTS

On or about September 4, 2009, the Securities & Exchange Commission issued to Spongetech a subpoena for documents that contained 94 identified categories and included documents relating to the operations of Spongetech, RM Enterprises, and the sale of its securities. Affirmation of Maranda Fritz ("Fritz Aff.") at Exhibit 1: SEC Subpoena. In or about October 2009, Spongetech responded to those broad requests, producing more than 30,000 pages. Fritz Aff. at Exhibit 2: Spongetech Response to SEC Subpoena.

The Affidavits submitted approximately six months later in support of the Application for Search Warrants for the office of Spongetech, and for Mr. Metter's home, make plain that those subpoenaed documents were then made available to the FBI. As reflected in those affidavits, the agents and the SEC had reviewed and analyzed those materials, and were seeking search warrants not to replicate that same expansive production but to secure particularized documents bearing on the criminal charges, including ones that post-dated Spongetech's document production. Fritz Aff. at Exhibit 3: McGuire Affidavit in Support of Search Warrant for 1 Tinker Lane; Fritz Aff. at Exhibit 5: Carrano Affidavit in Support of Search Warrant. Specifically,

Agent McGuire's affidavit in support of the warrant for Mr. Metter's home focused on the sales of Spongetech securities, and the opinion letters that facilitated those sales (Ex. 3 to Fritz Aff. at ¶¶ 4-21, 27-44). The Affidavit then described alleged structuring by individuals other than Mr. Metter. Ex. 3 to Fritz Aff. at ¶¶ 22-26. Finally, the Affidavit discussed a press release concerning new packaging and product lines (Ex. 3 to Fritz Aff. at ¶ 45), Spongetech's failure to file its 10K for FYE 2009, and continued trading of Spongetech stock. Ex. 3 to Fritz Aff. at ¶¶ 46-47. McGuire also described the fact that Mr. Metter had an office at his home, and stated that the agents had gone through his trash and found a sheet listing Spongetech's sales to Walmart and a listing of Walmart locations. Ex. 3 to Fritz Aff. at ¶ 51.

Agent McGuire then discussed, in boilerplate form, the kinds of issues that can arise in a search of electronic files, and requested permission to image and seize computer hardware and peripherals "to conduct an offsite search of the image or hardware for the evidence fruits [sic] and instrumentalities of violations" as described in Attachment A. Ex. 3 to Fritz Aff. at ¶ 58.

Attachment A to the search warrant, headed "Items to be Seized," consists of a list of 19 items. Ex. 4 to Fritz Aff. at Attachment A. Rather than reiterating the same broad requests contained in the SEC's subpoena relating to the entire universe of corporate documents, that Attachment A is focused on seven specific topics or categories of documents: documents concerning ownership, control, management, employees, income and expenses of Spongetech and RM Enterprises (Attachment A at ¶¶ a-c); documents regarding services provided by and transfers to and from Mr. Metter, Mr. Moskowitz, Mr. Lazauskas, and identified entities (Attachment A at ¶ i); documents concerning Spongetech's purchases, sales and customers (and purported customers) and the customer websites created by George Speranza (Attachment A at ¶¶ d-g); documents concerning its SEC filings (Attachment A at ¶ h); documents concerning its

promotional and marketing activities, its press releases, and its "stock promoters" (Attachment A at ¶¶ p-r); documents regarding sales of stock and opinion letters (Attachment A at ¶¶ j-l); and documents concerning specific "Beneficiaries" (Attachment A at ¶¶ m-n).

The Affidavit in support of the search warrant for the office of Spongetech was provided by IRS Agent John Carrano, and incorporates an affidavit of McGuire submitted in support of Arrest Warrants. With respect to the information relating to the operations of Spongetech, it appears substantially identical to McGuire's Affidavit. It too requests authorization to image and seize computer hard drives "and to conduct an offsite search of the image or hardware" for the evidence described in the warrant. Ex. 5 to Fritz Aff. at ¶ 60.

As of May 2010, the government seized a total of 63 hard drives from the offices of Spongetech and RM Enterprises. Fritz Aff. at Ex. 7: Chart of seized hard drives sketches of locations of seizures, Receipt from Tinker Lane. From the home of Mr. Metter, the government seized three hard drives including the one maintained by his wife, one Macbook computer, stock certificates of BusinessTalkRadio, Mr. Metter's employment agreement with BusinessTalkRadio, approximately $20,000 in cash, and Mr. Metter's personal financial records. Affidavit of Michael Metter at ¶ 2-4 & Ex. 7 to Fritz Aff.: Receipt from Tinker Lane.

Since then, the government has failed to conduct any forensic analysis to identify the electronic files that were within the scope of the warrant as opposed to those that were non-seizable. Instead, the government has repeatedly stated its intention *to simply disseminate to all defendants the entire contents of the seized hard drives*, without regard for whether the government was entitled to seize those materials in the first place, much less distribute them to others.

At a conference on November 22, 2010, the AUSA stated that the government intended to "provide the attorneys with copies of the computers that were seized." Fritz Aff. at Exhibit 10: Transcript 11/22/10 at 6.[4]

On January 25, 2011, the government provided an update to the court regarding the status of discovery.

At the conference that was held on February 4, 2011, the Court asked the government whether it was going to produce to the defense documents that it – the government – had not looked at. "How do you know its discoverable without looking at it.?" Fritz Aff. at Exhibit 11: Transcript 2/4/11 at 12. Later in the conference, AUSA Schaeffer again stated that "we intend to turn over to defense attorneys everything we seized before we look at it regardless of whether it has anything that might be privileged on it." The Court responded "So that I am 100% clear, the government is turning over all of these computer hard drives and documents without having reviewed it first yourselves?" Mr. Schaeffer responded "yes." Ex. 12: 2/4/11 Tr. at 24. The Court commented, "if they haven't looked at it, then they don't know what's on it." Counsel interposed its objection to the production of the entire contents of all hard drives to the entire assemblage of defendants. Ex. 12: 2/4/11 Tr. at 24-25, 27.

---

4 The government has not acknowledged that it was required to determine whether its seizures exceeded the scope of the warrants, but has acknowledged that it needs to conduct a privilege review. The government seemed to agree that it would set up a privilege team to locate privileged documents. Tr. at 7. According to the government, identification of privileged material was "a separate issue than discovery." Tr. at 7-8. The AUSA stated that he would be contacting each of the defense attorneys to "get a list of search terms so that we can process the computers." Tr. at 8. The list was provided on February 12, 2011. After the AUSA then objected to that list, and pressed for more information, counsel provided additional information in February relating to attorneys that may have provided legal advice.

Because the government represented that it would not be taking any steps to review the hard drives or filter out privileged or irrelevant materials, the defense asked that the hard drives be provided to the defendant who had used it prior to its wholesale production. Ex. 12: 2/4/11 Tr. at 28-29. Counsel could then object to the materials that are confidential, privileged or beyond the scope of the warrant.

The government objected, referring to the entirety of the contents of the hard drives as the "government's evidence" and claiming that "each defendant is entitled to review the Government's evidence to determine whether there's something in there they want to use." Ex. 12: 2/4/11 Tr. 29.

## ARGUMENT

## POINT I

## BECAUSE THE EXECUTION OF THE WARRANTS FOR SPONGETECH AND FOR METTER'S HOME WAS UNCONSTITUTIONAL, THE SEIZED MATERIALS SHOULD BE SUPPRESSED

### A. Authorities Relating to Seizures of Electronic Data

Courts have become increasingly concerned about ensuring that the government's ability to seize entire hard drives for off-site examination does not "become a vehicle" for a plainly unconstitutional "general" search.

> We recognize that overseizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which is has no probable cause to collect.

United States v. Comprehensive Drug Testing Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

The "overseizing" that will accompany seizure of a hard drive will often include not only irrelevant material but also personal non-seizable data.

> There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers.

United States v. Abdellatif, 2010 WL 5252852 at *5 (W.D.N.Y. 2010).

> The dawn of the Information Age has only heightened those [privacy] concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because '[c]omputers … often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize.

United States v. Cioffi, 668 F.Supp.2d 385, 391 (E.D.N.Y. 2009).

These issues involving computerized data have been addressed by the Department of Justice in its own publications. In discussing search warrants for electronic information, DOJ candidly acknowledges that computers "perform many functions" for its users, and "almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation." Ex. 12 to Fritz Aff.: *Department of Justice Computer Crime Manual* at 18 of 35.

It cannot be disputed that the government's indiscriminate seizure of materials that are beyond the scope of a warrant, and its retention of those items, requires suppression.[5] In United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), for example, agents seized and retained volumes of documents without ensuring that they were within the scope of the warrant. The court held that the government's retention of the documents for six months may have been "convenient," but was "an unreasonable and therefore unconstitutional manner of executing the warrant." *See also* United States v. Soliman, 2008 WL 4757300 at *8 (W.D.N.Y. Oct. 29, 2008) (ordering that government must "cull through" the seized materials and "identify and return those materials not covered by the warrant").

This issue was starkly presented in United States v. Debbi, 244 F.Supp.2d 235, 237 (S.D.N.Y. 2003). There, the government obtained search warrants that permitted seizure of items relating to allegations of obstruction of justice and health care fraud. Pursuant to that warrant, the agents seized electronic and paper files, financial and patient records.

---

[5] While the defendant bears the initial burden on a motion to suppress, "once the movant establishes some basis for the suppression motion, for example a search or seizure conducted without a warrant, the burden of proof shifts to the Government. The Government then carries the burden to demonstrate by a preponderance of the evidence that the search or seizure did not violate the Fourth Amendment." United States v. Murphy, 2011 WL 1518669 at *1 (W.D.N.Y. April 19, 2011) (citing United States v. Arboleda, 633 F.2d 985, 989 (2d Cir. 1980) & United States v. Allen, 289 F.Supp.2d 230, 242 (N.D.N.Y. 2003)).

Having seized items pursuant to the warrant, the government then failed to take any appropriate steps to separate that which was within the warrant from seized material that was plainly outside its scope. According to Judge Jed Rakoff, "the government essentially concedes that virtually no attempt was made at the time of the seizure itself to separate evidence of Debbi's alleged fraud and/or obstruction from other documents that were seized; that it was only after repeated demands from defense counsel, extending over months, that even a limited portion of improperly seized materials were returned (approximately one box); and that even after the instant motion was brought, no meaningful attempt was made to separate from what was actually seized the only items that the warrant permitted to be seized, i.e., evidence of Debbi's alleged fraud or obstruction." Even the court encouraged the government "to do the necessary sifting and return what was, by any measure, improperly seized." The Government did not do so, "rather lamely arguing that it was awaiting this Court's decision on the instant motion – as if, on any possible rationale, the Government would not be required to return what exceeded the plain limitation language of the warrant." Judge Rakoff stated:

> It is thus evident that the Government chose to blatantly disregard the very limitations that saved the warrant from overbreadth, and that the Government continues to do so. For all its protestations of good faith, the Government felt free to invade Debbi's home, seize his records without meaningful limitation and restraint, pick over them for months thereafter without determining which were actually evidence of the alleged crimes, and even now refrain from returning what it was never entitled to seize.

244 F.Supp.2d at 238. Based on that record, Judge Rakoff suppressed all seized materials that the Government had not yet determined to be within the scope of the warrant, and scheduled a hearing to determine whether all seized items should be suppressed. *See also* United States v. Squillacote, 221 F.3d 542, 556 (4th Cir. 2000), *cert. denied*, 532 U.S. 971 (2001) (as a general rule, when the seizure exceeds the scope of the warrant, the improperly seized evidence must be suppressed).

The more drastic remedy of "blanket suppression" of all seized evidence is justified when "the agent effected a widespread seizure of items not within the scope of the warrant and did not act in good faith." United States vs. Triumph Capital Group, 211 F.R.D. 31, 60 (D.Conn. 2002); United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000), *cert. denied* 534 U.S. 816 (2001). Where the agents acted with "flagrant disregard" of the limits of the warrant, all of the items seized may be suppressed. This issue typically arises where the agents have engaged in the "improper wholesale seizure of many items outside a warrant's scope," such that the process resembles a "general search."

> Government agents 'flagrantly disregard' the terms of a warrant so that wholesale suppression is required only when (1) they effect a 'widespread seizure of items that were not within the scope of the warrant.' and (2) do not act in good faith. … The rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search.

Liu, 239 F.3d at 140-41.

**B. The Government's Execution of the Spongetech & Metter Warrants was Unconstitutional**

The Affidavits in support of the Spongetech and Metter warrant, and the warrants themselves, relate to specific topics and appear sufficiently particularized.[6] Pursuant to the warrant, the government was authorized to seize documents that fell within the scope of that warrant, and obtained authorization to seize computer hard drives to then conduct appropriate searches to locate materials within the scope of the warrant. While those forensic steps are now fairly routine, the government declined to take those steps and instead repeatedly stated its

---

[6] Defendant Metter also moves for suppression of the materials seized from the home that were not within the scope of the warrant, including his laptop computer, his employment agreement with BTR, stock certificates of BTR, and approximately $27,000 in cash that had been kept in the home for years, since Mr. Metter was diagnosed with cancer, in case of emergency. Affidavit of Michael Metter at ¶¶ 2-4.

intention to disseminate to third parties the entire quantity of data that it had seized and retained.

The government's position here is a twofold violation of the terms of the warrant: first, it seized all of the hard drives from Spongetech but then failed to take the steps that were mandated by the warrant and that made that initial "overseizing" lawful. Remarkably, it not only seized documents without regard for whether they were within the scope of its authorization, but also then insisted that they could disseminate that material including that which it had no lawful right to seize in the first place.

While the government may respond by focusing on its ability to *initially* seize entire computer hard drives, that would be a dramatic distortion of the nature of that authorization. That authorization arose from judicial and legislative efforts to allow the government a reasonable opportunity ***to search data*** so as to comply with the scope of the warrant; it is not authorization to ignore the scope of the warrant.[7] *See* United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2000)(warrant authorized seizure of computer and then off site search); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999), *cert. denied*, 527 U.S. 1011 (1999) (warrant authorized seizure of computer and the subsequent off premises search). *See also* Fed.R.Crim.Pro, 41(e)(2)(b) Commentary (rule acknowledges need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant). And "the court must also consider whether the government's subsequent search of [defendant's] computers that it imaged

---

[7] The cases also discuss at length the procedures that are permissible in connection with the search of the hard drive, but those issues plainly do not exist here, where the government did not even undertake such a search and simply received and kept the entire contents of more than 60 hard drives. See United States v. Kernell, 2010 WL 1491873 (E.D Tenn. March 31, 2010), Report and Recommendation adopted by 2010 WL 1490921 (E.D.Tenn. April 13, 2010) (discussing permissibility of search procedures including areas that could be searched and search terms).

during the execution of the search warrant passes constitutional scrutiny." Dupree, 2011 WL 1004824 at *32. See United States v. Triumph Capital Group, 211 F.R.D. 31, 62 (D.Conn. 2002). Further, as acknowledged by DOJ, "[t]he Fourth Amendment does require that forensic analysis of a computer be conducted within a reasonable time." Ex. 12 to Fritz Aff. at 21 of 35. See United States v. Mutschelknaus, 564 F.Supp.2d 1072, 1077 (D.N.D. 2008), *aff'd*, 592 F.3d 826 (8th Cir. 2010).

While this jurisdiction and others have not yet required that search protocols be incorporated into the warrant, the courts have emphasized that they will scrutinize the treatment of "overseized" data to ensure that the government has performed searches designed to ensure compliance with a particularized warrant. *See* United States v. Graziano, 558 F.Supp.3d 304, 315 (E.D.N.Y. 2008) ("although the Second Circuit has not decided this precise issue, this Court declines to adopt a rule that would invalidate search warrants which do not contain a specific methodology explaining how the computers would be searched."); Borden v. United States, 2010 WL 2803969 at *7 (M.D.Fla. 2010).

> The Court emphasizes, however, that the rejection of the blanket rule [requiring search protocols] does not give law enforcement a license to turn every search of a computer into a general search; rather, there are Fourth Amendment limits to every search that apply with equal force to searches of computers. Thus, although courts are ill-suited to manage in advance how the computer will be searched, law enforcement must establish the basis for searching the computer and particularize the evidence being sought.

Graziano, 558 F.Supp.3d at 316.

The Graziano court went on to emphasize that "the manner of the execution of the warrant in searching the computer will also be subject to judicial review under a 'reasonableness' standard." Graziano, 558 F.Supp. at 316 (citing United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006)); United States v. Sage, 2007 WL 4592074 at *11 (W.D.Mo. Dec. 27, 2007). So long as the agent is using legitimate search methods, reasonably calculated to locate evidence within the

scope of the warrant, the search of the electronic files will be considered reasonable under the Fourth Amendment. *See* United States v. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007). See also Borden, *supra* (motion to suppress denied because "conscious effort was made to search only for information within limits of the search warrants; case agent testified that the imaged hard drives were searched to identify information within the scope of the search and agent then reviewed the list of those files and selected those for retention).

The "blanket suppression" of seized items is required where "government agents 'flagrantly disregard' the terms of a warrant. That flagrant disregard will be found "when (1) they effect of widespread seizure of items that were not within the scope of the warrant,'and (2) they do not act in good faith." United States v. Graziano, 558 F.Supp.2d 304, 309-10 (E.D.N.Y. 2008).

> As the Second Circuit has noted, 'the rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search.'

558 F.Supp.2d at 309.

Plainly, in this case, the government not only "overseized" but did so in dramatic fashion, taking virtually every hard drive in two office locations and from Mr. Metter's home. It did not then take the critical next step of identifying the material within the scope of the warrant, and returning that which was not properly seized. And so this Court is squarely confronted with the issue of whether the government's arguably cavalier treatment of the seized materials requires suppression.

Under these circumstances, and given the fact that the government remains unable to identify materials those materials that are within the scope of the warrant, the authorities support the view that the government did not comply with the warrant, and the seized electronic

materials should be suppressed. The government may argue, even at this late stage, that it should still be permitted to attempt to comply with the warrants by performing the required forensic analysis, and that it did not do so within a reasonable time frame because it was waiting to perform an attorney client review. Those arguments should be rejected. First, there exists no authority for the proposition that the delay in this case comports with a "reasonableness" standard, and if that is the government's position, the defense requests a hearing to explore the government's retention and handling of the seized materials. In fact, the government's repeated statements that the hard drives were "its evidence" and that it was going to simply produce all of that information to all defendants demonstrates that the government has not acknowledged any obligation to conduct the requisite examination to accomplish compliance with the warrant.

Second, the government appears to have "flagrantly" ignored the now fairly well established procedures for seizure and review of electronic data, which require diligent and good faith efforts to comply with a search warrant. Finally, the forensic analysis could and should have preceded the attorney client privilege review, since it would be done by those who possess technical expertise and are not a part of the trial team. See Cioffi, 668 F.Supp.2d at 392 (appropriate execution of warrant could include either description of search protocols in the warrant or "'firewalls' to prevent investigators and prosecutors from obtaining the results of a computer search until documents within the scope of the warrant had been segregated by a third party"). In light of these circumstances, and as in Debbi, the Court should order suppression of all of the seized electronic material, at least to the extent that the government has not yet confirmed that it is within the scope of the warrant.

## POINT II

## BECAUSE THE WARRANT FOR ALL CONTENTS OF MR. METTER'S EMAIL ACCOUNT WAS OVERBROAD, THE SEIZED MATERIALS SHOULD BE RETURNED AND SUPPRESSED

The government's seizure of Mr. Metter's email account implicates issues concerning particularity and probable cause rather than execution of the warrant. The issue, plainly presented here, is whether the government's allegations relating to Spongetech established probable cause for the wholesale seizure of years of Mr. Metter's entire personal email account, or whether that warrant was overbroad. Because the government sought the broadest imaginable warrant for this personal email account, without putting forth any adequate basis for a seizure of all of Mr. Metter's personal communications, the seized materials should be suppressed.

The validity of a warrant for personal email accounts depends, first, on whether the affidavit in support of the warrant sufficiently established the use of that email account in connection with and/or as an instrumentality of the alleged offense. United States v. Bowen, 689 F.Supp.2d 675, 682 (S.D.N.Y. 2010). Where, however, the affidavits fail to establish the use of the email account, or did not limit the seizure to emails related to the alleged crime, the seized materials should be suppressed. United States v. Cioffi, 668 F.Supp.2d 385 (E.D.N.Y. 2009).

The case most closely on point with this one, Cioffi, clearly supports the suppression of Mr. Metter's e-mail account. In fact, the argument for suppression in this case is even stronger, because the warrant in Cioffi was more tailored and narrow than the one in this case. The warrant in Cioffi sought emails for only a 10 month period, contained an Attachment A describing the "Service of Warrant and Search Procedure," and very explicitly sought authorization to seize only those "messages and content constituting evidence of violations of federal criminal law." The affidavit in Cioffi also confirmed that the searching authorities must

and would "examine all of the stored data to determine which of the files are evidence, fruits or instrumentalities of the crime."

The court in Cioffi held the warrant invalid on its face, because it did not "limit the items to be seized from Tannin's email account to emails constituting evidence of the crimes charges or indeed any crime at all. Nor did it attach and incorporate the Affidavit." Id. at 396.

Here, the government did not include in the warrant even the basic requirements that existed in Cioffi, and instead seized years of personal email based on the obviously false notion claim that "all" of Mr. Metter's personal email account constituted evidence of a crime. Exhibit 13 to Fritz Aff.: Cioffi Warrant Attachment A-1.

The affidavit submitted in support of that warrant fails to establish any basis for that unlimited seizure of an email account. It contains the same information concerning the alleged unlawful conduct relating to Spongetech, acknowledges that the email account of Mr. Metter is a personal one, and lists various examples of Spongetech-related emails that were sent from the personal account. It could not and does not claim that the account was used primarily for business.

This case, therefore, presents a circumstance that is more extreme even than Cioffi. The government's claims in this case involve particular areas of alleged misconduct in relation to the business, combined with the assertion that Mr. Metter has used his email account in relation to the business. But the government did not limit seizures to emails relating to Spongetech, it did not limit the seizure to evidence of the alleged offenses, it did not limit the seizure to the same categories of documents that were contained in the other search warrants. The government simply sought and obtained years worth of personal communications that are precisely the kinds of private materials that the Fourth Amendment is supposed to protect from invasion. And so the

Court is squarely confronted with the issue of whether, where there are alleged securities fraud violations, an individuals' entire personal email account – with all of its day to day family, confidential and even embarrassing contents – may properly be seized, examined and retained by the government. At the risk of sounding hyperbolic, if this seizure is permissible, then private and confidential communications – electronic or otherwise – are fair game for the government to seize, review at their leisure, and use if anything incriminating of any kind appears, without regard for an unlimited and arguably unprecedented invasion of privacy.

**Conclusion**

Based on the foregoing, the defendant respectfully submits that the seized electronic data, cash, and personal email account should be suppressed.

In the alternative, the defendant requests a hearing on the issue of the government's seizure and its retention of those materials.

DATED: New York, New York
May 25, 2011

HINSHAW & CULBERTSON LLP

By: *s/Maranda E. Fritz*

Maranda E. Fritz
780 Third Avenue, 4th Floor
New York, NY 10017
Tel: 212-471-6200
Fax: 212-935-1166